What is claimed is:

1. A method of providing an authentication service, comprising:

relating a user identity to a set of a plurality of authentication mechanisms;

relating a type of transaction with a relying party to a level of authentication; and

authenticating the user identity through at least one authentication mechanism in the set of the plurality of authentication mechanisms for the type of transaction, according to the level of authentication.

2. The method as recited in claim 1, further comprising:

selecting the at least one authentication mechanism depending on the plurality of authentication mechanisms related with the user and the level of authentication.

3. The method as recited in claim 1, further comprising:

monitoring a series of authentications for the relying party to detect fraud.

4. The method as recited in claim 1, wherein the authentication mechanisms in the set of authentication mechanisms are part of a distributed system.

5. The method as recited in claim 3, wherein at least one of the authentication mechanisms is mobile.

6. A computer-readable medium having computer-executable instructions for performing the method as recited in claim 1.

7. A method of syndication, comprising:

offering an authentication service, the authentication service being capable of authenticating a user identity with a plurality of authentication mechanisms, rendering results of the authentication to at least one relying party, and dynamically making an authorization decision; and

distributing the authentication service to the at least one relying party.

8. The method as recited in claim 7, wherein the at least one relying party integrates the authentication service together with other offerings.

9. The method as recited in claim 7, wherein the dynamic authorization decision is based on a requested access level, authentication mechanisms used, and an account status.

10. The method as recited in claim 7, further comprising:

providing secure recovery from potential fraud without requiring re-registration of a user.

11. The method as recited in claim 7, further comprising:

charging the relying party for each authenticating event.

12. A computer-readable medium having computer-executable instructions for performing the method as recited in claim 6.

13. A method of registration, comprising:

authenticating a user;

determining a level of identity confirmation for a registration;

receiving a new authentication mechanism;

receiving new authentication verification information; and

storing user identity information, the level of identity confirmation, and the new authentication verification information in a database.

14. The method as recited in claim 13, wherein authenticating the user is done by a registration server.

15. The method as recited in claim 13, wherein authenticating the user is done by a registration agent.

16. The method as recited in claim 13, wherein authenticating the user is performed by using an authentication mechanism stored in the database.

17. The method as recited in claim 13, further comprising:
receiving from the user, a request for registration.

18. The method as recited in claim 17, wherein receiving the request for registration is done by an authentication server.

19. The method as recited in claim 17, wherein receiving the request for registration is done by an authentication agent.

20. The method as recited in claim 13, wherein determining the level of identity confirmation for the registration is done by a registration server.

21. The method as recited in claim 13, wherein determining the level of identity confirmation for the registration is done by a registration agent.

22. The method as recited in claim 13, wherein receiving new authentication verification information is done by a registration server.

23. The method as recited in claim 13, further comprising sending the user identity information, the level of identity confirmation, and the new authentication verification information.

24. The method as recited in claim 23, wherein sending is done from a registration server to an authentication server.

25. The method as recited in claim 23, wherein sending the user identity information, the level of identity confirmation, and the authentication verification information is done from a registration agent to a registration server.

26. The method as recited in claim 23, further comprising sending pre-existing user information.

27. A method of providing an authentication service, comprising:

providing a list of supported authentication methods;

receiving requirements for an authentication level from at least one relying party;

receiving a selection of authentication methods from at least one user;

receiving identification information for the at least one user;

producing a portfolio associated with the at least one user, the portfolio comprising the list of authentication methods, each authentication method in the portfolio meeting the selection of the at least one user, each authentication method in the portfolio supported by an authentication system, the list of authentication methods meeting the requirements for the authentication level from the at least one relying party; and

relating the identification information to the portfolio for the at least one user.

28. The method as recited in claim 27, wherein receiving the selection is a subset of the list of supported authentication methods.

29. The method as recited in claim 27, further comprising:

storing the portfolio on an authentication server capable of providing the authentication service to the at least one relying party.

30. The method as recited in claim 27, further comprising:

providing a selection of authentication methods to the at least one user;

receiving at least one selected authentication method from the at least one user;

receiving authentication information required to perform authentication for each of the at least one selected authentication methods;

wherein the portfolio includes the authentication information.

31. The method as recited in claim 27, further comprising:

authenticating, by the authentication system, the at least one user to the at least one relying party.

32. The method as recited in claim 31, wherein authenticating the at least one user to the at least one relying party comprises:

providing a challenge to the at least one user;

accepting a response to the challenge from the at least one user;

examining the response to the challenge to ensure its authenticity;

comparing authentication information received by the at least one user to the portfolio associated with the at least one user; and

communicating an authentication result to the at least one relying party.

33. The method as recited in claim 27, wherein the at least one relying party is an online pharmacy and the at least one user is a doctor.

34. The method as recited in claim 27, further comprising:

adding a new authentication method to the portfolio.

35. The method as recited in claim 34, wherein adding the new authentication method to the portfolio comprises:

authenticating the at least one user using an authentication method already in the portfolio;

receiving authentication information for the new authentication method; and

storing the new authentication method and its authentication information in the portfolio.

36. The method as recited in claim 27, further comprising:

receiving notice of a potentially compromised authentication method in the portfolio;

authenticating the at least one user using an authentication method already in the portfolio, but not using the potentially compromised authentication method; and

revoking the authentication information for the potentially compromised authentication method in the portfolio associated with the at least one user.

37. The method as recited in claim 27, further comprising:

monitoring authentication events for the at least one user; and

detecting possible fraud for a suspect authentication method.

38. The method as recited in claim 37, further comprising:

authenticating the at least one user using an authentication method already in the portfolio, but not using the suspect authentication method;

communicating the possible fraud to the at least one user; and

upon confirmation of fraud, revoking the suspect authentication method in the portfolio.

39. The method as recited in claim 37, further comprising:

automatically revoking the suspect authentication method in the portfolio;

wherein the possible fraud is potentially serious fraud.

40. A computer-readable medium having computer-executable instructions for performing the method as recited in claim 27.

41. A method of authentication, comprising:

requesting, by a user to a relying party, a protected service;

sending, by the relying party, a description of the request to an authorization server;

determining, by the authorization server, a first level of assurance;

sending, by the authorization server to an authentication server, the first level of assurance;

requesting, by an authentication server, authentication from the user;

entering, by the user, authentication information into an authentication device;

sending, by the authentication device to the authentication server, authentication information;

verifying, by the authentication server, the authentication information using authentication verification information stored in a portfolio in a database that is associated with the user;

computing, by the authentication server, a second level of assurance;

evaluating whether the second level of assurance is high enough;

sending, by the authentication server to the authorization server, a first success message, upon determining the second level of assurance is high enough;

verifying, by the authorization server, information from the authentication server;

verifying, by the authorization server, that the user is allowed to perform the protected service;

sending, by the authorization server to the relying party, a second success message, upon verification of the information from the authentication server and verification that the user is allowed to perform the protected service; and

providing, by the relying party to the user, the protected service.

42. The method as recited in claim 41, further comprising:

requesting, by the authentication server to the user, authentication using at least one additional authentication method, upon determining the second level of assurance is not high enough.

43. The method as recited in claim 42, further comprising:

sending, by the authentication server to the authorization server, a first failure message and a reduced level of assurance, upon determining the user is unable to authenticate using the at least one additional authentication method;

storing, by the authorization server, the reduced level of assurance;

sending, by the authorization server to the relying party, a second failure message; and

providing, by the relying party to the user, a third failure message.